Attachment B

Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *OneDrive content.* The contents of all files, passwords, and keys and other records stored in any OneDrive account associated with the Subject Account, including all Windows operating system device backups;

b. *Microsoft Account content*: The contents of all files, passwords, and keys and other records stored in any Microsoft Account associated with the Subject Account;

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

Information to be seized by the government

1. All records in the accounts described in Attachment A that relate to the following federal crimes involving Gregory Davis and Serhat Gumrukcu: murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1); kidnapping, in violation of 18 U.S.C. § 1201; wire

fraud, in violation of 18 U.S.C. § 1343; and murder for hire, in violation of 18 U.S.C. § 1958, including:

a. any and all data related to Gregory Davis, including his personal identifiers, address, residence, vehicles, and businesses;

b. any and all data related to the death of Gregory Davis, including information related to efforts to locate his whereabouts prior to his murder;

c. any and all data related to communications involving Jerry Banks, Aron Ethridge, Berk Eratay, Murat Gumrukcu, and Serhat Gumrukcu from January 1, 2015 to the present;

d. any and all data relating to Serhat Gumrukcu's business activity from January 1, 2015 to May 2022, including all data relating to businesses associated with Serhat Gumrukcu, such as Enochian Bioscience.

e. any and all data relating to Serhat Gumrukcu's criminal case charged by the State of California in February 2017;

f. any and all data relating to the schedule, travel or location of Serhat Gumrukcu, Murat Gumrukcu, Berk Eratay and Aron Ethridge from January 1, 2017 to July 1, 2018, and from April 6, 2022 to the present; and

g. any and all bank records, checks, credit card bills, account information, and other financial records relating to Berk Eratay's employment, earnings, and finances.

2. Evidence of user attribution showing who used or owned the account at the time the things described in this warrant were created, edited, or deleted.

3. All records or other information regarding the identification of the Subject Account, to include full name, physical address, telephone numbers, email addresses (including

primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the Subject Account was created, the length of service, the IP address used to register the Subject Account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

4. All records or other information regarding the devices associated with, or used in connection with, the Subject Account (including all current and past trusted or authorized Windows OS devices and computers, and any devices used to access Microsoft services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");
5. All records pertaining to the types of Microsoft services used in connection with the Subject Account;
6. All records pertaining to communications between Microsoft and any person regarding the Subject Account, including contacts with support services and records of actions taken;
7. All BitLocker recovery keys stored in any OneDrive account associated with the Subject Account; and

8. All BitLocker recovery keys stored in any Microsoft Account associated with the Subject Account.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.